Remarks/Arguments

Claims 1-20 are pending.

Objection to the Specification

Responsive to the objection to the title, the title has been replaced with "Method for Managing Access between a Service Provider and a Set-Top Box in a Conditional Access System." Applicants submit that the replacement title is sufficiently descriptive of the invention.

Objection to claim 9 under 35 USC 112, second paragraph.

Responsive to the objection to claim 9, claim 8 has been amended to depend from claim 7. Applicants submit that the phrase "said second identification data" in claim 9 now has proper antecedent basis.

Rejection of claims 1-7 and 10 under 35 USC 103(a) as being unpatentable over "Applied Cryptography" ("Schneier").

Applicants respectfully traverse this rejection in part, and deem the rejection overcome in part, for at least the following reasons.

35 U.S.C. §103(a) sets forth in part:

> [a] patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.

To establish a prima facie case of obviousness, all of the recited claim limitations must be taught or suggested in the prior art. *See, MPEP 2143.03; see also, In re. Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974).* Further, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine reference teachings. *See, M.P.E.P. 706.02(j).* Further yet, the teaching or suggestion to make the claimed combination must be found in the prior art, and not based on the applicant's own disclosure. *In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).*

In this case, Applicants respectfully submit that the Examiner has selectively picked various elements from Schneier, without sufficient justification for such a combination, to derive the claimed invention and that such a proposed combination constitutes impermissible hindsight reconstruction.

Initially, the examiner cites the description of a basic authentication protocol using public-key cryptography. However, the examiner acknowledges that the protocol as described in Schneier does not disclose the use of a digital certificate to secure a key K. To provide the missing element, the examiner cites a different section of Schneier that describes using a digital certificate to secure a public key that is used to decrypt an encrypted principle message.

However, the examiner fails to provide the required teaching or suggestion for the combination, and merely states that "it would be obvious to one of ordinary skill in the art at the time the invention was made for the decrypting key (public key of node B) of the encrypted principle message to be secured by a certificate. Motivation for such an implementation would enable node A to ensure that B's public key and B's subject identification information are valid since the information is verified by a trusted third party as taught by Schneier." However, such a statement merely states the result arising from the combination.

Further, the examiner acknowledges that the proposed combination still fails to disclose the step of node A submitting the original principle message to node B. To provide the missing element, the examiner cites yet another section of Schneier that describes a challenge protocol. As justification for the combination the examiner states "It would be obvious to one of ordinary skill in the art at the time the invention was made to use the principle message as a challenge value to authenticate the identity of node B and the timeliness of the message received from node B. **Motivation for such an implementation would enable node A to authenticate node B using standard challenge means as taught by Schneier.** (emphasis added)" Again, such a statement merely restates the result that would arise from the proposed combination, not why the reference suggests that such a combination is desirable.

Finally, the examiner states that the modified scheme discloses a final authentication step of A sending to B a third encrypted message comprising the data of B's identification garnered from B's digital certificate and encrypted using A's private key wherein B decrypts the third encrypted message using A's public key. The examiner then asserts that this final step is effectively equivalent to the third encrypted message being encrypted by A using B's public key garnered from B's digital signature wherein B decrypts the third encrypted message using B's private key. Applicants respectfully disagree and submit that these are two different and distinct uses of a public key cryptosystem. The first scenario allows B to "authenticate" that the message was sent by A since the message is encrypted with A's private key. However, second scenario allows B to decrypt the message but does not allow authentication since the message is encrypted with B's public key.

In view of the above, Applicants respectfully submit that the rejection is based on impermissible hindsight reconstruction that picks and chooses elements described in the Schneier reference without sufficient support for the proposed combination. Therefore, Applicants submit that present claims 1-7 and 10 are patentably distinguishable over the teachings of the Schneier.

Rejection of claims 8, 9 and 11 under 35 USC 103(a) as being unpatentable over "Applied Cryptography" ("Schneier") and further in view of Arnold (US Patent No. 5,78,172).

Applicants respectfully submit that for at least the reasons discussed below present claims 8, 9 and 11 are patentably distinguishable over the teachings of Schneier in view of Arnold.

Present claim 11 recites

"... (b) **receiving from the smart card**, in response to said first message, a first digital certificate encrypted using a first private key, **said first digital certificate containing service provider identification data**;

(c) authenticating the smart card in response to said first digital certificate;

(d) **contacting the service provider in response to the authentication of the smart card and said service provider identification data** and sending a second message to the service provider, said second message containing set-top box identification data... (emphasis added)"

Claim 8 has been amended to recite similar features. Support for the recitation is provided, for example, in page 9, lines 2-5. Applicants submit that nowhere do the combination of Schneier and Arnold teach or suggest such features.

The examiner acknowledges that Schneier is silent on the matter of managing access between a service provider and a set-top box with a smart card. Arnold is cited as disclosing a method for authenticating a cryptographic link between a service provider and a set-top box using a smart card coupled thereto by means of certificate authentication (Figures 1 and 7A-7C and related text). However, Arnold fails to teach or suggest the above cited features of claims 11 and 8.

Arnold shows in Fig. 7C the steps for registration of a decoder box (DEC) by a entitlement control system (ECS-RS). In that regard, a decoder according to Arnold does not use service provider identification data provided via the smart card to contact the service provider. Rather, according to Arnold the ECS-RS contacts the DEC and provides the necessary data for DEC to contact and register with the ECS-RS. See, for example, col. 28, line 59 - col. 29, line 10:

> *At a process block 762, the ECS 108 sends a "register here" message to the head end 114 over the communication line 132.* ***This message will contain a telephone number for the ECS-RS 110 and information about the location of the head end 114 or UL 112 from which the message was received.*** *At a process block 764, the head end 114 and the UL 112 repetitively send the "register here" message to the decoders 116, 118 over the communications lines 134, 128, 136, 138. In the preferred embodiment*

> *, a decoder 116, 118 that has not yet been registered cannot understand any message or data that it receives, except for the "register here" message because all other information is encrypted, and the decoder 116, 118 does not yet have the necessary keys to decrypt any of the information. At a process block 766,* ***the decoder 116, 118 establishes a telephone link with the ECS-RS 110 over the communications line 130, 131 using the telephone number obtained from the "register here" message.*** (emphasis added).

Thus, it is clear that Arnold fails to teach or suggest notable features recited in present claim 11 and amended claim 8. Therefore, Applicants submit that claims 8, 9 and 11 are patentably distinguishable over the combination of Schneier and Arnold.

Rejection of claims 12-20 under 35 USC 103(a) as being unpatentable over "Applied Cryptography" ("Schneier"), in view of Arnold (US Patent No. 5,78,172), and further in view of Force et al. (US Patent No. 5,533,123).

Applicants respectfully submit that for at least the reasons discussed below present claims 8, 9 and 11 are patentably distinguishable over the teachings of Schneier in view of Arnold and in further view of Force.

Regarding claim 12, Force is cited as disclosing a smart card having a plurality of certificates, each certificate identifying a distinct service. However, the teachings of Force fail to cure the defect of Schneier and Arnold with respect to claim 11 as discussed above. Therefore, Applicants submit that claim 12, which depends from claim 11, is patentably distinguishable over the combination of Schneier, Arnold and Force.

The Office Action states that claims 13-20 are method claims that correspond to claims 1-12, and as such, they are rejected for the same reasons as those set forth for claims 1-12. Applicants note that claims 13-20 depend from claim 11, which recites the additional features cited above. These features are not recited in claims 1-7. Further, nowhere does Force cure the defect of Schneier and Arnold with respect to claim 11 as discussed above. Therefore, Applicants submit that claims 13-20 are patentably distinguishable over the combination of Schneier, Arnold and Force.

Having fully addressed the Examiner's rejections it is believed that, in view of the preceding amendments and remarks, this application stands in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited. If, however, the Examiner is of the opinion that such action cannot be taken, the Examiner is invited to contact the applicant's attorney at (609) 734-6815, so that a mutually convenient date and time for a telephonic interview may be scheduled.

Respectfully submitted,
Ahmet M. Eskicioglu, et al.

By: Paul P. Kiel
Attorney for Applicants
Registration No. 40,677

THOMSON Licensing Inc.
PO Box 5312
Princeton, NJ 08543-5312

Date: Sept 3, 2004

CERTIFICATE OF MAILING

I hereby certify that this amendment is being deposited with the United States Postal Service as First Class Mail, postage prepaid, in an envelope addressed to Mail Stop Amendment, Commissioner for Patents, Alexandria, Virginia 22313-1450 on:

9/3/04
Date

Eliza Buchalczyk